



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
17.04.2002 Bulletin 2002/16

(51) Int Cl.7: **G06F 1/00**

(21) Application number: **00120390.0**

(22) Date of filing: **18.09.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
 Designated Extension States:
AL LT LV MK RO SI

(72) Inventor: **Ikeda, Hidetaka**
1-1-1 Shibaura, Minato-ku Tokyo 105-8001 (JP)

(74) Representative:
Blumbach, Kramer & Partner GbR
Radeckestrasse 43
81245 München (DE)

(71) Applicant: **KABUSHIKI KAISHA TOSHIBA**
Kawasaki-shi, Kanagawa-ken 210-8572 (JP)

(54) **Secured portable electronic device**

(57) The present invention is provided with a base board (2) on which wiring is provided, a memory (4), installed on the base board (2) by soldering, for storing data and a certification key, and a memory control LSI (3). The memory control LSI is a fabricated as a bare chip incorporating an internal memory (3b) for storing data and a certification key, and a control section (3a) for controlling the storing of data in the memory (4) and

the reproduction of the data from the memory (4). The bare chip is installed on the base board (2) and covered with sealing resin. The bare chip is connected to the base board (2) by gold wire bonding. The certification key stored in the memory (4) is compared with the certification key stored in the internal memory. Based on the coincidence or non-coincidence between these keys, the control section determines whether or not the memory (4) is an intended one.

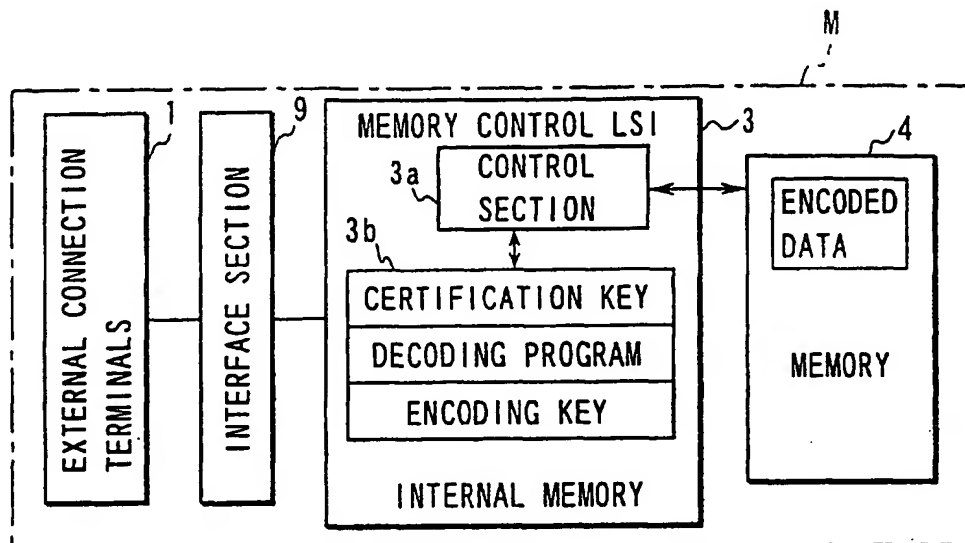


FIG. 14

Description

[0001] The present invention relates to a portable electronic medium which functions as a memory card, and in which a memory for storing data and a control circuit for controlling the memory are independently installed on the same card.

[0002] Where a memory for storing data and a control circuit (a control LSI) for controlling the memory are independently installed on the same card (a base board), it is general that they are soldered to the base board.

[0003] Owing to this structure, the memory can be easily replaced with a new one, and the control LSI can be detached for analysis.

[0004] In other words, a counterfeit can be made by merely replacing only the memory with another, or by increasing the storage capacity.

[0005] The present invention has been made in consideration of the above circumstances, and is intended to prevent the installation of a memory that does not correspond to the control circuit in use, thereby preventing fabrication of a counterfeit employing such a memory.

[0006] The present invention is also intended to prevent easy analysis of the control circuit in use.

[0007] According to the present invention, there is provided a portable electronic medium comprising: a base board on which wiring is provided; a first memory, installed on the base board, for storing data and a first certification key; and a control circuit including: a second memory for storing data and a second certification key; and a control section for controlling an operation of storing data in the first memory and an operation of reading the data from the first memory, the second memory and the control section being fabricated as a chip which is installed on the base board and connected to the base board, the control section checking whether the first certification key stored in the first memory coincides with the second certification key stored in the second memory, thereby determining whether or not the first memory is an intended one.

[0008] According to the present invention, there is also provided a portable electronic medium comprising: a base board on which wiring is provided; a first memory, installed on the base board, for storing data; and a control circuit including: a second memory for storing data and a first-memory-state information; and a control section for controlling an operation of storing data in the first memory and an operation of reading the data from the first memory, the second memory and the control section being fabricated as a chip which is installed on the base board and connected to the base board, the control section checking whether the first memory is in a state coinciding with first-memory-state information stored in the second memory, thereby determining whether or not the first memory is an intended one.

[0009] According to the present invention, there is further provided a portable electronic medium comprising: a base board on which wiring is provided; a first memory,

installed on the base board, for storing data and encoded data obtained by encoding a first certification key; and a control circuit including: a second memory for storing data, a second certification key, an encoding key, and a decoding program; and a control section for controlling an operation of storing data in the first memory and an operation of reproducing the data from the first memory, the second memory and the control section being fabricated as a chip which is installed on the base board and connected to the base board, the control section decoding the encoded data stored in the first memory by use of the encoding key and decoding program stored in the second memory, and further checking whether a resultant certification key coincides with the certification key stored in the second memory, thereby determining whether or not the first memory is an intended one.

[0010] This summary of the invention does not necessarily describe all necessary features so that the invention may also be a sub-combination of these described features.

[0011] The invention can be more fully understood from the following detailed description when taken in conjunction with the accompanying drawings, in which:

FIG. 1 shows the internal structure of a memory card according to the present invention.

FIG. 2 shows the internal structure of the memory card.

FIG. 3 shows a sectional structure of the memory card.

FIG. 4 shows the internal structure of the memory card.

FIG. 5 is a control block diagram of the memory card.

FIG. 6 shows an example of a manner in which a certification key is stored according to the first embodiment.

FIG. 7 is a flow chart illustrating the processing that is performed when the memory card of the first embodiment is actuated or when power supply voltage is applied.

FIG. 8 shows an example of a manner in which a certification key is stored according to the first embodiment.

FIG. 9 shows an example of a manner in which memory state information are stored according to the second embodiment.

FIG. 10 is a flowchart illustrating how certification processing is performed according to the second embodiment.

FIG. 11 shows how music information edited at the end of the last-time processing is stored in the memory of the memory card according to the second embodiment.

FIG. 12 is a flowchart illustrating how memory state information are stored and certification processing is performed according to the second embodiment.

FIG. 13 shows how memory state information are stored in an internal memory according to the second embodiment.

FIG. 14 shows how encoded data, a certification key, an encoding key and a decoding program are stored according to the third embodiment.

FIG. 15 is a flowchart illustrating how certification processing is performed according to the third embodiment.

FIG. 16 shows how encoded data, a certification key, an encoding key and a decoding program are stored according to the third embodiment.

FIG. 17 shows how encoded data, a certification key, an encoding key, a decoding program and an encoding program are stored according to the fourth embodiment.

FIG. 18 is a flowchart illustrating how certification processing is performed according to the fourth embodiment.

FIG. 19 shows how encoded data, a certification key, an encoding key, a decoding program and an encoding program are stored according to the fourth embodiment.

FIG. 20 shows the entire Internet connection system according to the fifth embodiment.

FIG. 21 illustrates how the Internet connection system of the fifth embodiment is used in a volume-sales store so as to register Internet connection information in a memory card.

[0012] Embodiments of the present invention will now be described.

[0013] FIGS. 1 to 3 show the structure of a memory card M (an SD card), which is an example of a portable electronic medium. FIG. 1 shows the internal structure of the memory card M according to the present invention, FIG. 2 also shows the internal structure of the memory card M, and FIG. 3 shows a sectional structure of the memory card.

[0014] The memory card M comprises a base board 2 provided with external connection terminals 1.

A memory control LSI (a control circuit, a controller) 3, a memory (an external memory, a first memory) 4, chip components 5, and ICs of other types are installed on the base board 2. As shown in FIG. 4, the memory card is received in a case 7.

[0015] The external connection terminals 1 of the base board 2 are coated with a hard gold plating layer, so as to improve the contact-resistant characteristic.

[0016] The base board is coated with a soft gold plating layer on the surface 2a that is reverse to the surface where the external connection terminals 1 are provided.

[0017] On surface 2a, the memory control LSI 3 (which is a bare chip for memory control) is die-bonded. The base memory control LSI 3 is connected to the base board by gold wire bonding and is covered with sealing resin 8. Thereafter, the memory 4, which is of a TSOP type, the chip components 5 and the ICs are installed

by soldering.

[0018] Since the memory control LSI 3 is installed on the base board 2 by bare chip installation, the key data cannot be easily analyzed.

[0019] The control circuit of the memory card M will be described with reference to FIG. 5.

[0020] As shown in FIG. 5, the memory card M is made up of: external connection terminals 1 through which data are exchanged with reference to an external apparatus (not shown); an interface section 9 connected to the external connection terminals 1; a memory control LSI 3 connected to the interface section 9; and the memory 4, connected to the memory control LSI 3, for controlling the storing/reproduction of data. The interface section 9 is made of chip components 5 and ICs 6.

[0021] The memory control LSI 3 includes a control section 3a for controlling the entire memory, and an internal memory (a second memory) 3b for storing a control program and data.

[0022] When the memory card M is connected to the external apparatus (not shown), power supply voltage is applied thereto.

[First Embodiment]

[0023] A description will be given of an embodiment wherein the memory 4 is certified by use of the certification key unalterably stored in the internal memory 3b and the certification key unalterably stored in the memory 4.

[0024] A unique value serving as a certification key is stored in the internal memory 3b, as shown in FIG. 6. The value is unalterably stored.

[0025] Each of the memory 4 and the internal memory 3b is made up of an unalterable ROM portion and an alterable ROM portion. The certification key is stored in the unalterable ROM portion.

[0026] With reference to the flowchart shown in FIG. 7, a description will be given of the processing that is performed when the memory card of the first embodiment is actuated or when power supply voltage is applied.

[0027] First of all, the control section 3a executes a self check (ST 1) when the card is actuated or when a power supply voltage is applied from the external apparatus. If the self check shows "OK" in step (ST 2), the control section 3a reads out the certification key from the memory 4 (ST 3), and further reads out the certification key from the internal memory 3b (ST 4). Then, the control section 3a compares the two keys, for coincidence (ST 5).

[0028] If the comparison shows that the two keys coincide with each other, the control section 3a certifies the memory 4 (certification "OK") (ST 6). Then, the control section 3a is set in the standby state (ST 7).

[0029] If the self-check in step ST 2 indicates "NG" or if the certification of step S6 indicates "NG", the control section 3a stops processing (ST 8).

[0030] If step 2 shows that the certification is "NG", this means that the comparison in step 5 indicates the key discrepancy and the memory 4 is not the certified one.

[0031] In the above, reference was made to the case where the memory 4 is certified when the card is actuated or when the power supply voltage is applied to the external apparatus. It should be noted, however, that the memory may be certified in a similar manner each time it is accessed.

[0032] The memory 4 may be accessed when music information or a program externally supplied is stored, or when the music information or program stored in the memory 4 is reproduced or executed.

[0033] The certification key, which is stored in the internal memory 3b for certification of the memory 4, may be used for certifying the relationship between the external apparatus and the card M. As shown in FIG. 8, moreover, the internal certification key K1 for certifying the memory 4 and the external certification key K2 for certifying the external apparatus can be stored in the internal memory 3b of the card M.

[Second Embodiment]

[0034] By use of the above structure, the memory control LSI 13 can store the state of the memory 4 (i.e., the manner of processing). When the memory 4 is accessed next, the state information, which indicate the state of the memory 4, are checked to see whether or not they remain the same since the last-time access. Based on this check, the memory 4 is certified.

[0035] In the case of the second embodiment, the control section 3a stores the state information on the memory 4 in the internal memory 3b when the processing using the memory card M comes to an end, as shown in FIG. 9. The state information on the memory 4 include: the area used at the last processing (FAT: a file allocation table); a check sum of the whole of the memory 4 (a verification value); a check sum stored in the memory 4 at the end of the last-time processing (a verification value); etc. By this storing, the internal memory 3b stores information regarding the area used at the last processing (FAT: a file allocation table); a check sum of the whole of the memory 4 (a verification value); a check sum stored in the memory 4 at the end of the last-time processing (a verification value); or the like.

[0036] The memory 4 described above is a nonvolatile memory and can retain the state in which the memory 4 is in the last-time processing. The internal memory 3b is also a nonvolatile memory and can hold state information on the memory 4.

[0037] A description will be given as to how certification processing is performed when the memory 4 is accessed by use of the above structure. In the description below, the flowchart shown in FIG. 10 will be referred to.

[0038] The memory 4 may be accessed when music information or a program externally supplied is stored,

or when the music information or program stored in the memory 4 is reproduced or executed.

[0039] When the memory 4 is to be accessed, the control section 3a checks the storing state of the memory 4 (ST 11) and determines which area (FAT) was used in the last-time processing (ST 12). Then, the control section 3a compares this area (FAT), i.e., the area determined as having been used in the last-time processing, with the area (FAT) registered in the memory 3b as having been used in the last-time processing (ST 13).

[0040] If the comparison shows that the two areas coincident with each other, the control section 3a determines that the memory 4 is certified (certification "OK") (ST 14). Then, the access processing to the memory 4 is started (ST 15). The access processing is, for example, the storing (writing) of data, or the reproduction (reading) of stored data.

[0041] After the execution of the access processing, the control section 3a stores the data indicating the area (FAT) used for the access processing in the internal memory 3b (overwrite) (ST 16).

[0042] If the comparison in step ST 16 indicates the area discrepancy, the control section 3a determines that the certification is "NG" and therefore ends the access processing (ST 17).

[0043] In the above description, reference was made to a FAT as indicating the state information on the memory 4. Needless to say, the check sum of the whole of the memory 4 (a verification value), a check sum stored in the memory 4 at the end of the last-time processing (a verification value) or the like may be used in a similar manner.

[0044] Let us assume a case where at the end of the last-time processing, music information "A" are stored in address "AAAA" of the memory 4 to have length of "BB", as shown in FIG. 11. A description will be given as to how, in this case, the processing for storing the memory state information and the certification processing are executed, with reference to the flowchart shown in FIG. 12.

[0045] First of all, the control section 3a calculates a check sum "CC" (a verification value) corresponding to the music information "A" (ST 21).

[0046] Subsequently, the control section 3a generates memory state information (ST 22) by adding the following three to the information ID originally provided for the music information "A": (i) the storing start address "AAAA" of the memory 4; (ii) the length "BB" of the stored information; and (iii) the check sum "CC" (a verification value) calculated as above. The memory state information, thus generated, are stored in the internal memory 3b (ST 23), as shown in FIG. 13.

[0047] When the memory 4 is about to be accessed (ST 24), the control section 3a confirms the stored state of the memory 4 (ST 25) and determines that information having a length of "BB" were stored in address "AAAA" of the memory 4 at the end of the last-time processing (ST 26).

[0048] Then, the control section 3a calculates the check sum "CC" (a verification value) corresponding to the information that starts from address "AAAA" of the memory 4 and has a length of "BB" (ST 27).

[0049] On the basis of the address "AAAA", the length "BB" and the calculated check sum "CC" (a verification value), the control section 3a determines memory status information (ST 28). The memory state information are compared with the memory state information read out from the internal memory 3b and used in the last-time processing so as to see whether they coincide with each other (ST 29).

[0050] If the comparison indicates coincidence of information, the control section 3a certifies the memory 4 (certification "OK") (ST 30) and executes the accessing processing to the memory 4 (ST 31).

[0051] If the comparison in step 29 indicates a discrepancy of information, the control section 3a determines that the certification is "NG" and ends the access processing (ST 32).

[Thlrd Embodiment]

[0052] A description will now be given of an embodiment wherein the memory 4 is certified by using: encoding data for the certification key unalterably stored in the memory 4; the certification key unalterably stored in the internal memory 3b; the decoding program; and the encoding key.

[0053] In the case of this embodiment, the memory 4 stores encoded data obtained by encoding a certification key by use of a unique certification key, as shown in FIG. 14. The encoded data are unalterably stored.

[0054] As shown in FIG. 14, the internal memory 3b stores a certification key that is identical to the certification key used before the encoding of the encoded data stored in the memory, a decoding program used for decoding the encoded data stored in the memory 4, and an encoding key used when the encoded data are decoded in accordance with the decoding program. The keys and program are stored unalterably.

[0055] Each of the memory 4 and the internal memory 3b is made up of an unalterable ROM portion and an alterable ROM portion. The certification key is stored in the unalterable ROM portion.

[0056] A description will be given, with reference to the flowchart shown in FIG. 15, as to how the memory 4 is certified by use of the structure described above.

[0057] First of all, the control section 3a reads out the encoded data from the memory 4 (ST 41). Then, the control section 3a decodes readout encoded data in accordance with the encoding key stored in the internal memory 3b. For this decoding operation, the decoding program stored in the internal memory 3b is executed. As a result, a certification key is obtained (ST 42). Further, the control section 3a compares that certification key with the certification key stored in the internal memory 3b (ST 43), for coincidence.

[0058] If the comparison indicates coincidence between the certification keys, the control section 3a certifies the memory 4 (certification "OK") (ST 44).

[0059] If the comparison in step 43 indicates a discrepancy, the control section 3a determines that the certification is "NG" (ST 45).

[0060] The certification key, which is stored in the internal memory 3b for certification of the memory 4, may be used for certifying the relationship between the external apparatus and the card M. As shown in FIG. 16, moreover, the internal certification key K1 for certifying the memory 4 and the external certification key K2 for certifying the external apparatus can be stored in the internal memory 3b of the card M.

[Fourth Embodiment]

[0061] A description will now be given of an embodiment wherein the memory 4 is certified by executing both the certification processing (steps 41-45) of the third embodiment and the certification processing (steps 11-14) of the second embodiment. The memory 4 is certified when data are received from an external apparatus and stored in the memory 4.

[0062] In the case of the fourth embodiment, encoded data, which are obtained by encoding a certification key in accordance with a unique encoding key, are stored beforehand, as shown in FIG. 17. The encoded data are unalterably stored.

[0063] As shown in FIG. 17, the internal memory 3b stores a certification key that is identical to the certification key used before the encoding of the encoded data stored in the memory 4, an encoding program used for encoding reception data received from the external apparatus, a decoding program used for decoding the encoded data stored in the memory 4, and an encoding key used when the reception data are encoded in accordance with the encoding program or when the encoded data are decoded in accordance with the decoding program. The keys and programs are stored unalterably.

[0064] As shown in FIG. 17, the internal memory 3b information regarding the area used at the last processing (FAT: a file allocation table); a check sum of the whole of the memory 4 (a verification value); a check sum stored in the memory 4 at the end of the last-time processing; or the like.

[0065] Each of the memory 4 and the internal memory 3b is made up of an unalterable ROM portion and an alterable ROM portion. The certification key is stored in the unalterable ROM portion. The alterable ROM portion is a nonvolatile memory and retains the state in which the memory 4 is in the last-time processing.

[0066] A description will be given, with reference to the flowchart shown in FIG. 18, as to how the certification processing is executed upon reception of data from the external apparatus by use of the structure described above.

[0067] Upon reception of data from the external apparatus (ST 51), the control section 3a executes the certification processing (ST 52) according to the third embodiment, and further executes the certification processing (ST 53) according to the second embodiment.

[0068] If each certification processing is "OK" (ST 54), the control section 3a encodes the received data (ST 55) in accordance with the encoding key stored in the internal memory 3b. For this encoding operation, the encoding program stored in the internal memory 3b is executed.

[0069] Then, the control section 3a stores the encoded data in the memory 4 (ST 56).

[0070] After this storing operation, the control section 3a stores the data indicating the state of the memory 4 in the internal memory 3b (overwrite) (ST 57).

[0071] If either certification processing is "NG", the control section 3a ends the processing (ST 58).

[0072] When the encoded data stored in the memory 4 is decoded for reproduction, the decoding operation is performed in a similar manner to that described above.

[0073] The data to be stored in the memory 4 may be music information or a program.

[0074] The certification key, which is stored in the internal memory 3b for certification of the memory 4, may be used for certifying the relationship between the external apparatus and the card M. As shown in FIG. 19, moreover, the internal certification key K1 for certifying the memory 4 and the external certification key K2 for certifying the external apparatus can be stored in the internal memory 3b of the card M.

[Fifth Embodiment]

[0075] A description will now be given of a manner in which a memory card M having the certification function described above is used.

[0076] By way of example, how the memory card M is employed in an internet connection system will be described with reference to FIGS. 20 and 21.

[0077] FIG. 20 shows the internet connection system to which the memory card M capable of certifying an incorporated memory is applied.

[0078] Referring to FIG. 20, each of electronic devices, such as a PC (personal computer) 11, a cellular phone (or a mobile phone) 12, an electronic camera and a TV (television) set 14, is provided with a card slot and a communication interface (not shown). The card slot is designed to receive a memory card M which is substantially equal in size to a postage stamp. The memory card M includes a hidden storage area which cannot be externally accessed. The communication interface is required for connection to the Internet 15, etc., and an example of the communication interface is a modem.

[0079] According to the present embodiment, the memory 4 of the memory card M stores Internet connection

information 150, including a user ID, a user password, a mail account, a mail password, a DNS server address, an access point (a telephone number for access), etc. The data format of the Internet connection information 150 registered in the memory 4 of the memory card M is predetermined without reference to the types of electronic devices (namely, the PC 11, cellular phone 12, electronic camera 13 and the TV set 14 described above).

[0080] When a memory card M is inserted in the card slot, the PC 11 is automatically booted up and reads out the Internet connection information 150 of the predetermined format from the memory 4 of the card M. This memory 4 stores an application program 110 used for automatic connection to the Internet 15 (i.e., an Internet connection setting application program 110). When the memory card M is actuated, the processing for certifying an incorporated memory, i.e., the processing described in relation to the first, second and third embodiments, is executed. When the memory certification is "OK", the PC 11 (i.e., an external apparatus) can be certified by using the certification key stored in the memory 3b of the memory card M. When these certifications are "OK", the application program is executed.

[0081] The cellular phone 12, electronic camera 13, TV set 14 and other electronic devices are also provided with a storage medium that is readable by a computer. The storage medium stores an Internet connection setting application program (hereinafter referred to simply as an "application"). The storage medium is made of a ROM, a disk drive, a flash memory, etc. The application 110 may be downloaded through a communication line.

[0082] As described above, each of the electronic devices (the PC 11, the cellular phone 12, the electronic camera 13, etc.) is provided with an application (i.e., an Internet connection setting application). With this structure, what is required of the user is merely to carry the memory card M, the memory 4 of which stores the Internet connection information 150, and insert it in the card slot of an arbitrary one of the electronic devices (namely, the PC 11, the cellular phone 12, the electronic camera 13 or the TV set). By so doing, connection to the Internet 15 can be easily established. The memory card M is not designed to be dependent on any specific one of the electronic devices. In other words, the user can choose an electronic device to be used, and insert the memory card M in the card slot of the chosen device. By merely doing so, the user can be connected to the Internet through the device.

[0083] In connection with this embodiment, a description will be given of a shop that registers the Internet connection information 150 in the memory 4 of the memory card M. A customer (i.e., the user) takes a memory card M to the shop or buys one from the shop. Then, the customer asks the shop to register the Internet connection information in the memory 4 of the memory card M. In the case illustrated in FIG. 20, a volume-sales store 16 and a convenience store 27 register the Internet connection

nection information. For this registration, a PC 160 in the volume-sales store 16 is provided with a computer-readable storing medium, and this storing medium stores information 180 used for the registration of Internet connection information (i.e., an Internet connection information registration application program). The convenience store 17 is provided with an information write terminal 170, and the storing medium of this terminal 170 stores not only an application used for registering Internet connection information in the memory 4 of the memory card M (i.e., an Internet connection information-registration application) but also an application used for downloading digital contents to the memory card M or an MD (i.e., a mini-disk).

[0084] In this manner, the volume-sales store 16 and the convenience store 17 serve as service shops that can register Internet connection information. Owing to the registration service by these shops, users (subscribers) who made a contract with Internet providers 18 (hereinafter referred to simply as providers) can be counted according to the providers 18 or the service shops. Each provider 18 can therefore give a refund 19 to a system provider (i.e., a company that provides an Internet connection system using a portable storing medium) or the service shops (i.e., the shops that registers Internet connection information, such as the volume-sales shop 16 and convenience store 17) in accordance with the number of subscribers 19.

[0085] A description will now be given as to how the Internet connection information registration service shop registers (writes) Internet connection information in the memory 4 of the memory card M by use of the system shown in FIG. 20. In the following below, FIG. 21 will be referred to.

[0086] When the memory card of the user is inserted in the card slot of the PC 160, as indicated by arrow a, the Internet connection information-registration application 180 is started. A list of providers (a provider list menu) 201 is shown on the display unit of the PC 160. (The providers make a contract with the company that provides the system shown in FIG. 20.)

[0087] On the provider list menu 201, the user selects a provider or a salesperson of the volume-sales store 16 selects one provide the provider requested by the user. In response to this selection, the PC 160 executes the application 180 and displays a message 202 indicating subscriber contract contents corresponding to the selected provider. A confirmation button 202a is included in the menu, and when the confirmation button is pushed (selected), a payment method selection menu 203 is displayed. When a payment method is selected on this menu, then a mail account preparation menu 204 is displayed. After mail accounts desired by the user are entered, the PC 160 is connected to the server 210 of the provider designated by the user (the connection is established through the Internet). The payment method and mail accounts desired by the user are therefore sent to the server 210. A confirmation request is subsequent-

ly made, as indicated by arrow b, and an online confirmation message 205 is displayed.

[0088] The server 210 of the provider designated by the user checks the mail accounts desired by the user to see whether they have been already assigned to another user. This check is made in the order of the first to third choices. If one of the mail accounts has not yet been assigned, it is determined that the mail account in question is assigned to the user. If all mail accounts have been already been assigned, the server 210 requests that different mail accounts be entered from the PC 160 of the volume-sales shop 16.

[0089] After determining a mail account desired by the user and assigning it to the user, the server 210 determines a user ID, a user password and a mail password, which are to be assigned to the user. The information on these are transmitted to the PC 160 of the volume-sales store 16, along with the information required for the Internet connection, including a DNS server address and an access point.

[0090] On the basis of the information transmitted from the server 210 of the provider, the PC 160 of the volume-sales store 16 generates Internet connection information 150 of predetermined format. The Internet connection information include a user ID, a user password, a mail password, a DNS server address, and an access point. The Internet connection information 150 are encoded according to a predetermined algorithm by use of a media key, which will be described below. When the operation for writing the encoded information in the memory 4 of the memory card M inserted in the card slot of the PC 160 has been started, a message 206 is displayed, indicating that information are being written.

[0091] When information are written in the memory 4 of the memory card M, the certification according to the fourth embodiment is executed. When the memory certification is "OK", the PC 11 (i.e., an external apparatus) can be certified by using the certification key stored in the memory 3b of the memory card M. When these certifications are "OK", the write operation is started.

[0092] After writing the Internet connection information 150 in the memory 4 of the memory card M, the PC 160 displays an inquiry message 207, asking the user whether or not to protect the information in the memory card M by use of a password.

[0093] If the protection based on a password is asked for, the PC 160 prompts the user to designate a password. Then, the PC 160 encodes the password designated by the user in accordance with a predetermined algorithm, and stores it in the memory card M. This encoded password is used as a key for taking out a media key from the memory card M. By writing the password in the memory card M, the PC 160 completes a series of operations for writing the Internet connection information, i.e., the user registration processing. Thereafter, the PC 160 displays a message 208 indicating the completion of user registration, and notifies a contract count server 211 of the completion of user registration through

the Internet, as indicated by arrow c. The contract count server 211 is owned by the business proprietor that developed the present system (i.e., the system providing company). On the other hand, if the protection based on a password is not asked for, the PC 160 immediately displays the user registration completion message 208 and notifies the contract count server 211 of the user registration completion, as indicated by arrow c. The notification of the contract count server includes the transmission of the information regarding the provider with which the user made a contract.

[0094] The contract count server 211 stores the data on the number of users (subscribers) who made a contract with Internet providers, and the number of users is counted according to the providers or the Internet connection information registration service shops. Each time a notice of user registration completion is received from the PC 160 of the volume-sales shop 16, the contract count server 211 increases the number of subscribers to a provider by one, and the volume-sales shop 16 (i.e., the shop that performed the service of registering the Internet connection information for the connection to that provider) increases the number of subscribers by one.

[0095] As described above, data used as a key is written in an area of a memory, so as to prevent the fabrication of a counterfeit memory card. The memory control LSI certifies the key data, and access to the memory is allowed only when coincidence is detected.

[0096] Even if the memory of the memory card is replaced with a memory of greater storage capacity, the certification by the memory control LSI does not indicate coincidence, and access to the memory is therefore prevented.

[0097] To prevent analysis, the key data in the memory can be encoded.

[0098] The present invention relates to a memory card comprising: a memory for storing data; a control section for controlling the storing of data in the memory or controlling the reproduction of the data from the memory; and a memory control LSI including an internal memory used by the control section. The control section compares the certification key stored in the memory with the certification key stored in the internal memory, and determines coincidence or non-coincidence. Based on this determination, the memory is certified.

Claims

1. A portable electronic medium characterized by comprising:

a base board (2) on which wiring is provided;
a first memory (4), installed on the base board (2), for storing data and a first certification key;
and
a control circuit (3) including: a second memory

(3b) for storing data and a second certification key; and a control section (3a) for controlling an operation of storing data in the first memory (4) and an operation of reading the data from the first memory (4), said second memory (3b) and said control section (3) being fabricated as a chip which is installed on the base board (2) and connected to the base board (2),

said control section (3a) checking whether the first certification key stored in the first memory (4) coincides with the second certification key stored in the second memory (3b), thereby determining whether or not the first memory (4) is an intended one.

2. A portable electronic medium according to claim 1, characterized in that:

said first memory (4) is installed on the base board (2) by soldering; and
said second memory (3b) is a bare chip installed on the base board (2).

3. A portable electronic medium according to claim 1, characterized in that said first and second memories (4, 3b) store the second certification keys in an unalterable manner.

4. A portable electronic medium according to claim 1, characterized in that said first and second memories (4, 3b) include ROM portions, respectively, and the certification keys are stored in the ROM portions.

5. A portable electronic medium according to claim 1, characterized in that:

said first memory (4) and said control circuit (3) are installed on one surface of the base board (2); and
an external connection terminal, coated with a hard gold layer, is provided on another surface of the base board (2).

6. A portable electronic medium according to claim 1, characterized in that said second memory (3b) stores a control program for controlling the control section (3a).

7. A portable electronic medium characterized by comprising:

a base board (2) on which wiring is provided;
a first memory (4), installed on the base board (2), for storing data; and
a control circuit (3) including: a second memory (3b) for storing data and a first-memory-state

Information; and a control section (3a) for controlling an operation of storing data in the first memory (4) and an operation of reading the data from the first memory (4), said second memory (3b) and said control section (3a) being fabricated as a chip which is installed on the base board (2) and connected to the base board (2),

said control section (3a) checking whether the first memory (4) is in a state coinciding with first-memory-state information stored in the second memory (3b), thereby determining whether or not the first memory (4) is an intended one.

8. A portable electronic medium according to claim 7, characterized in that:

said first memory (4) is installed on the base board (2) by soldering; and
said second memory (3b) is a bare chip installed on the base board (2).

9. A portable electronic medium according to claim 7, characterized in that said first and second memories (4, 3b) are nonvolatile memories.

10. A portable electronic medium according to claim 7, characterized in that said first memory (4) is a nonvolatile memory, and said second memory (3b) includes a nonvolatile memory portion in which the first-memory-state information are stored.

11. A portable electronic medium according to claim 7, characterized in that:

said first memory (4) and said control circuit (3) are installed on one surface of the base board (2); and
an external connection terminal, coated with a hard gold layer, is provided on another surface of the base board (2).

12. A portable electronic medium according to claim 7, characterized in that said second memory (3b) stores a control program for controlling the control section (3a).

13. A portable electronic medium according to claim 7, characterized in that said first-memory-state information include at least one of: information indicating which area of the first memory (4) is used at last-time processing; a verification value used at the end of the last-time processing; and a verification value regarding entity of the first memory (4).

14. A portable electronic medium according to claim 13, characterized in that said area of the first memory (4) is defined by a start address and a data length.

15. A portable electronic medium characterized by comprising:

a base board (2) on which wiring is provided; a first memory (4), installed on the base board (2), for storing data and encoded data obtained by encoding a first certification key; and a control circuit (3) including: a second memory (3b) for storing data, a second certification key, an encoding key, and a decoding program; and a control section (3a) for controlling an operation of storing data in the first memory (4) and an operation of reproducing the data from the first memory (4), said second memory (3b) and said control section (3a) being fabricated as a chip which is installed on the base board (2) and connected to the base board (2),

said control section (3a) decoding the encoded data stored in the first memory (4) by use of the encoding key and decoding program stored in the second memory (3b), and further checking whether a resultant certification key coincides with the certification key stored in the second memory (3b), thereby determining whether or not the first memory (4) is an intended one.

16. A portable electronic medium according to claim 15, characterized in that:

said first memory (4) is installed on the base board (2) by soldering; and
said second memory (3b) is a bare chip installed on the base board (2).

17. A portable electronic medium according to claim 15, characterized in that said first and second memories (4, 3b) are nonvolatile memories.

18. A portable electronic medium according to claim 15, characterized in that said first and second memories (4, 3b) include nonvolatile memory portions, the nonvolatile memory portion of the first memory (4) stores said encoded data, and the nonvolatile memory portion of the second memory (3b) stores said certification key, said encoding key, and said decoding program.

19. A portable electronic medium according to claim 15, characterized in that:

said first memory (4) and said control circuit (3) are installed on one surface of the base board (2); and
an external connection terminal, coated with a hard gold layer, is provided on another surface of the base board (2).

20. A portable electronic medium according to claim 15, characterized in that said second memory (4, 3b) stores a control program for controlling the control section (3a).

5

10

15

20

25

30

35

40

45

50

55

10

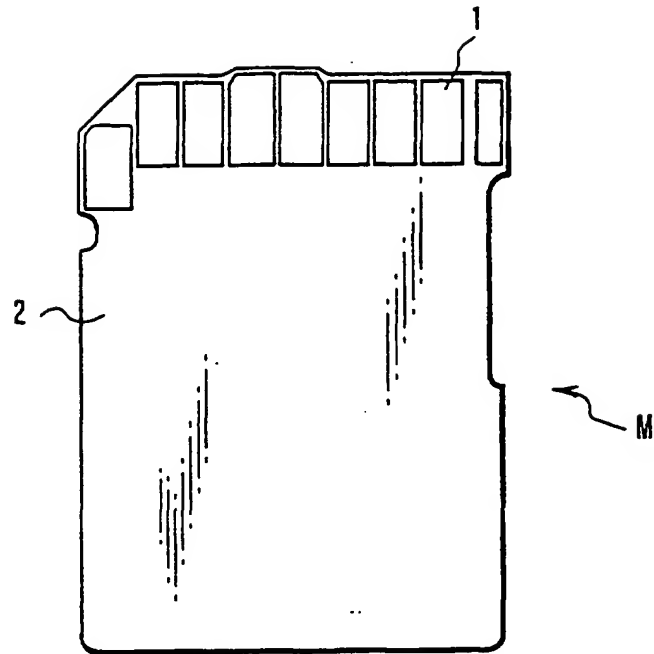


FIG. 1

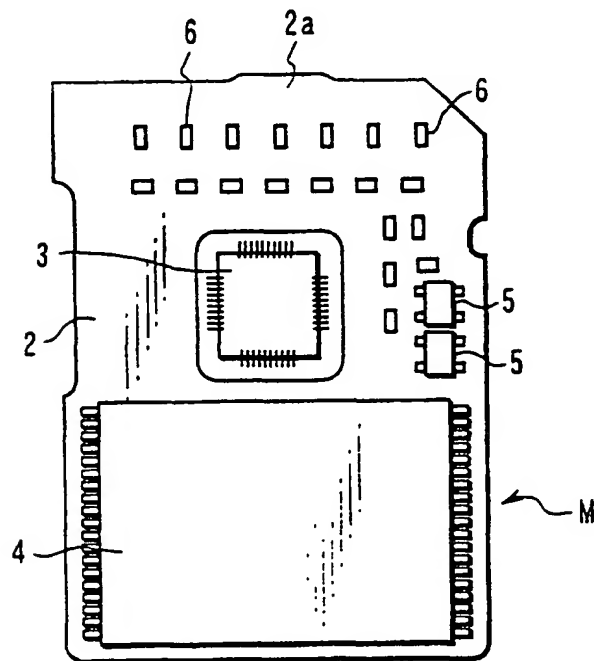


FIG. 2

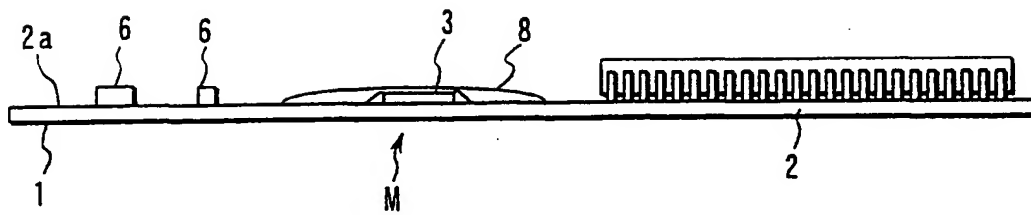


FIG. 3

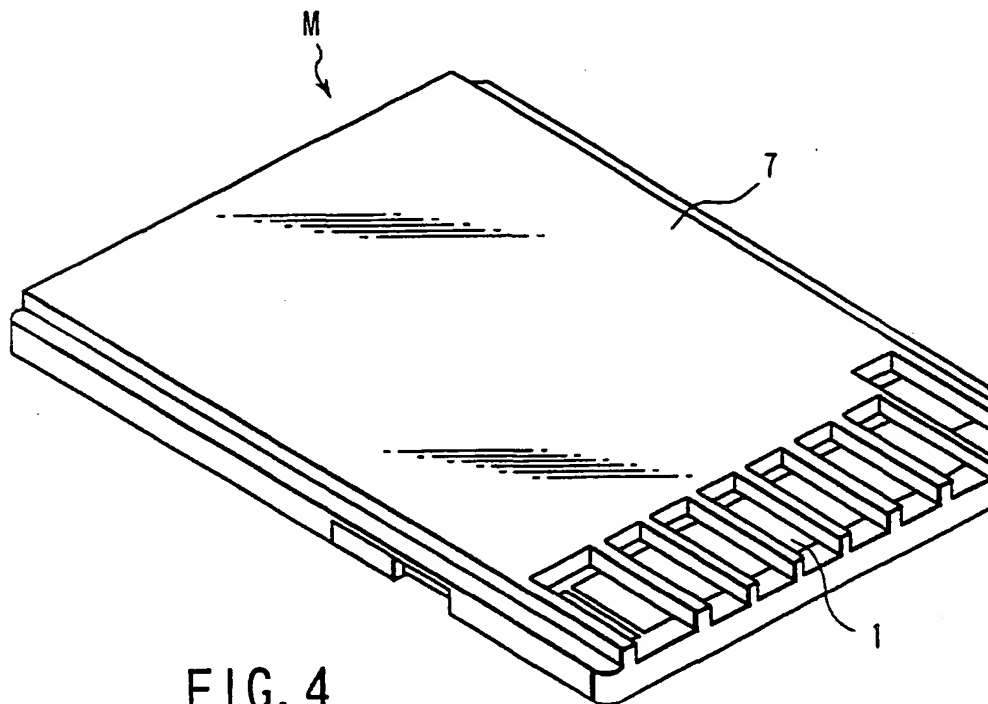


FIG. 4

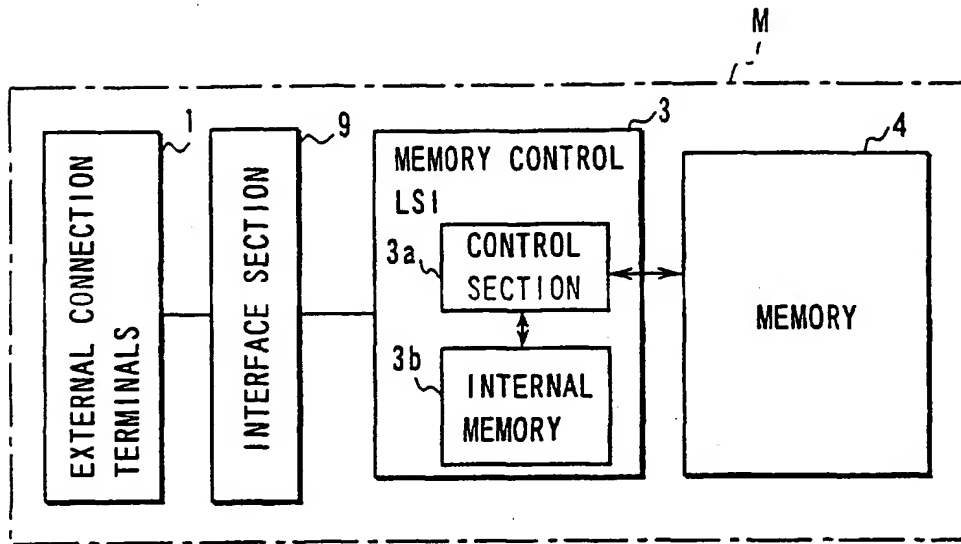


FIG. 5

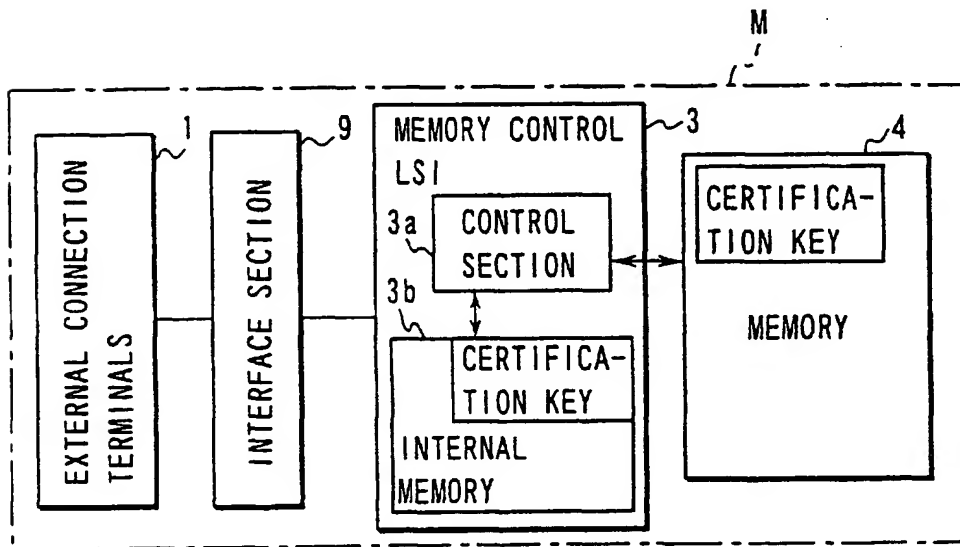
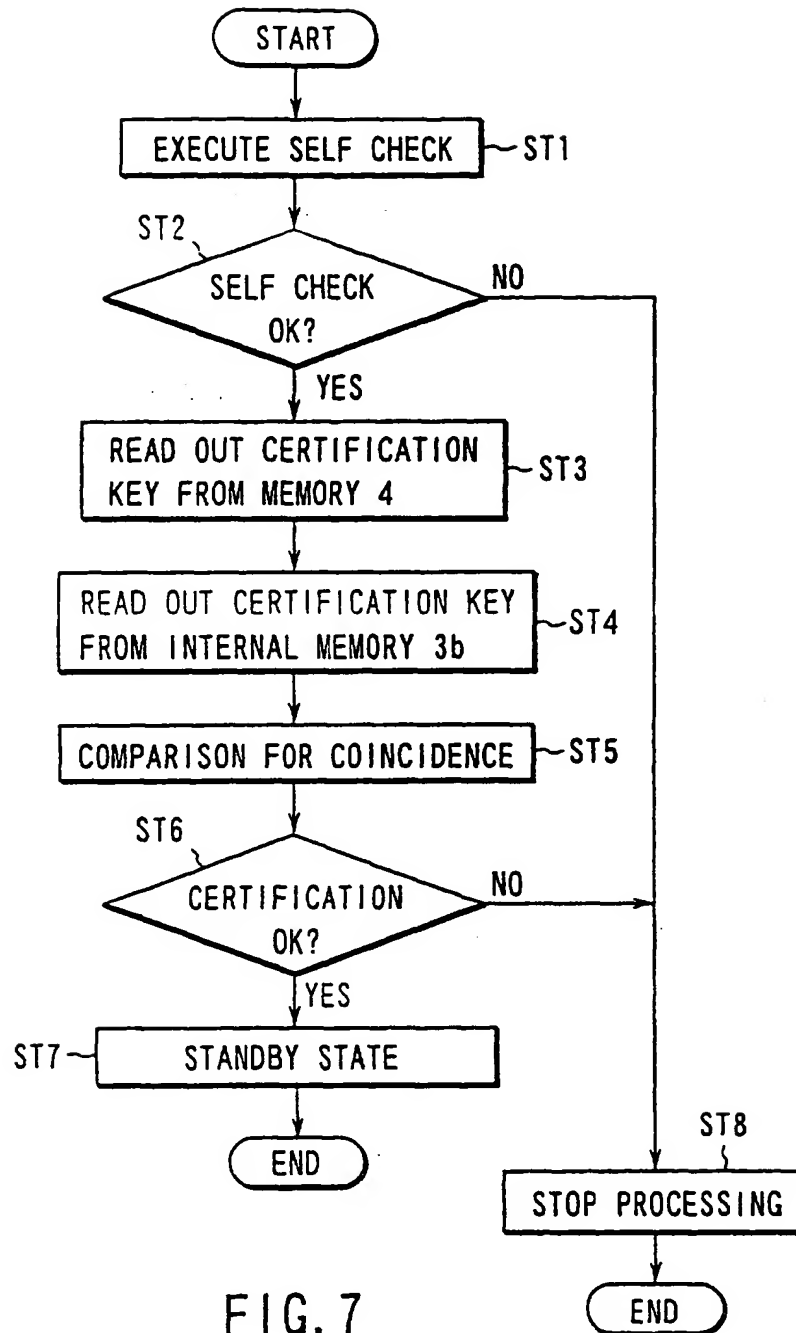


FIG. 6



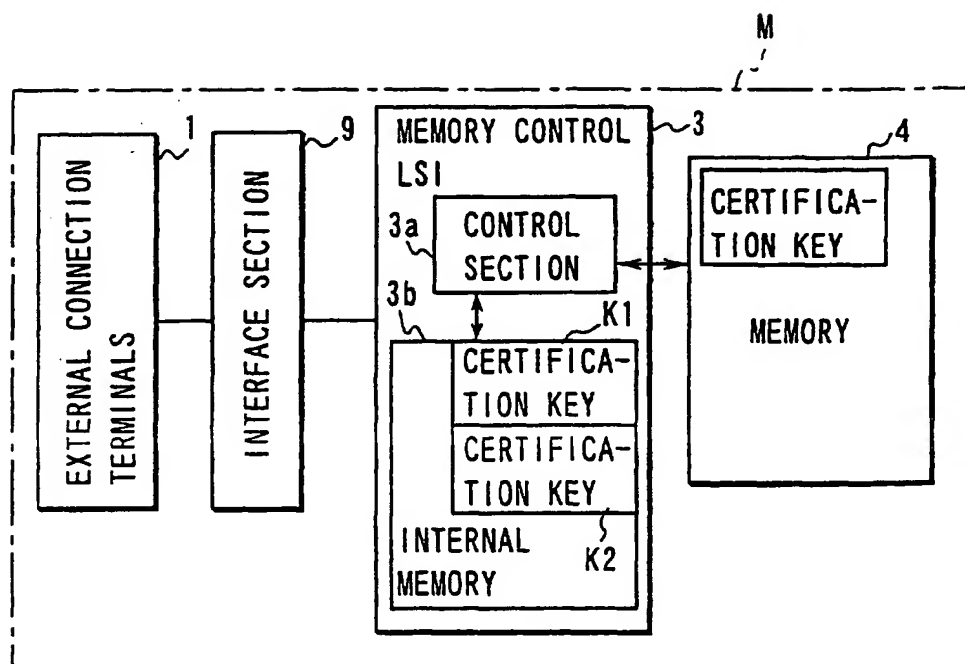


FIG. 8

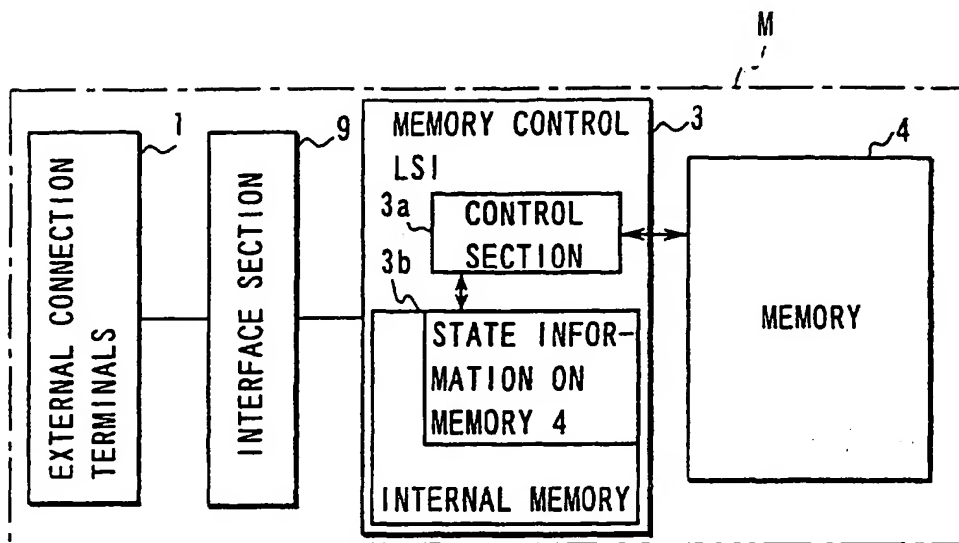


FIG. 9

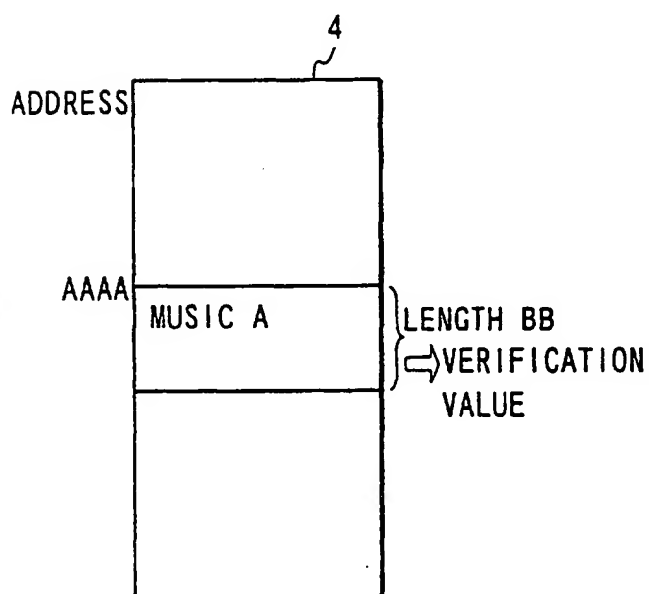


FIG. 11

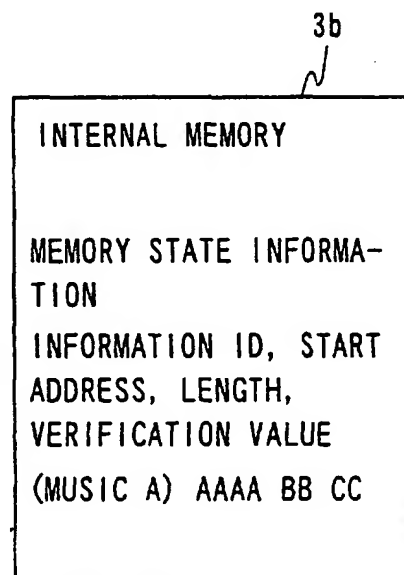


FIG. 13

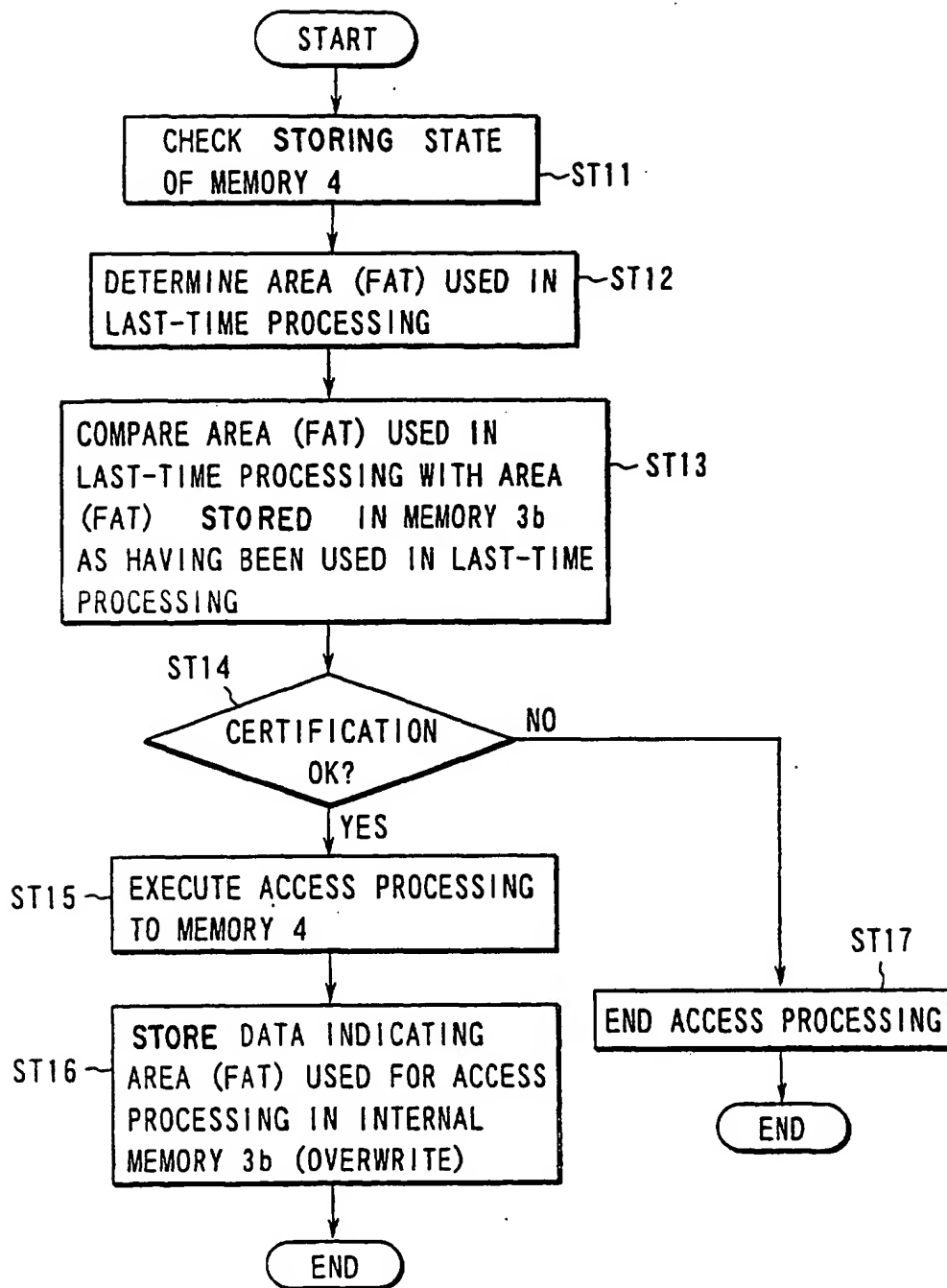


FIG. 10

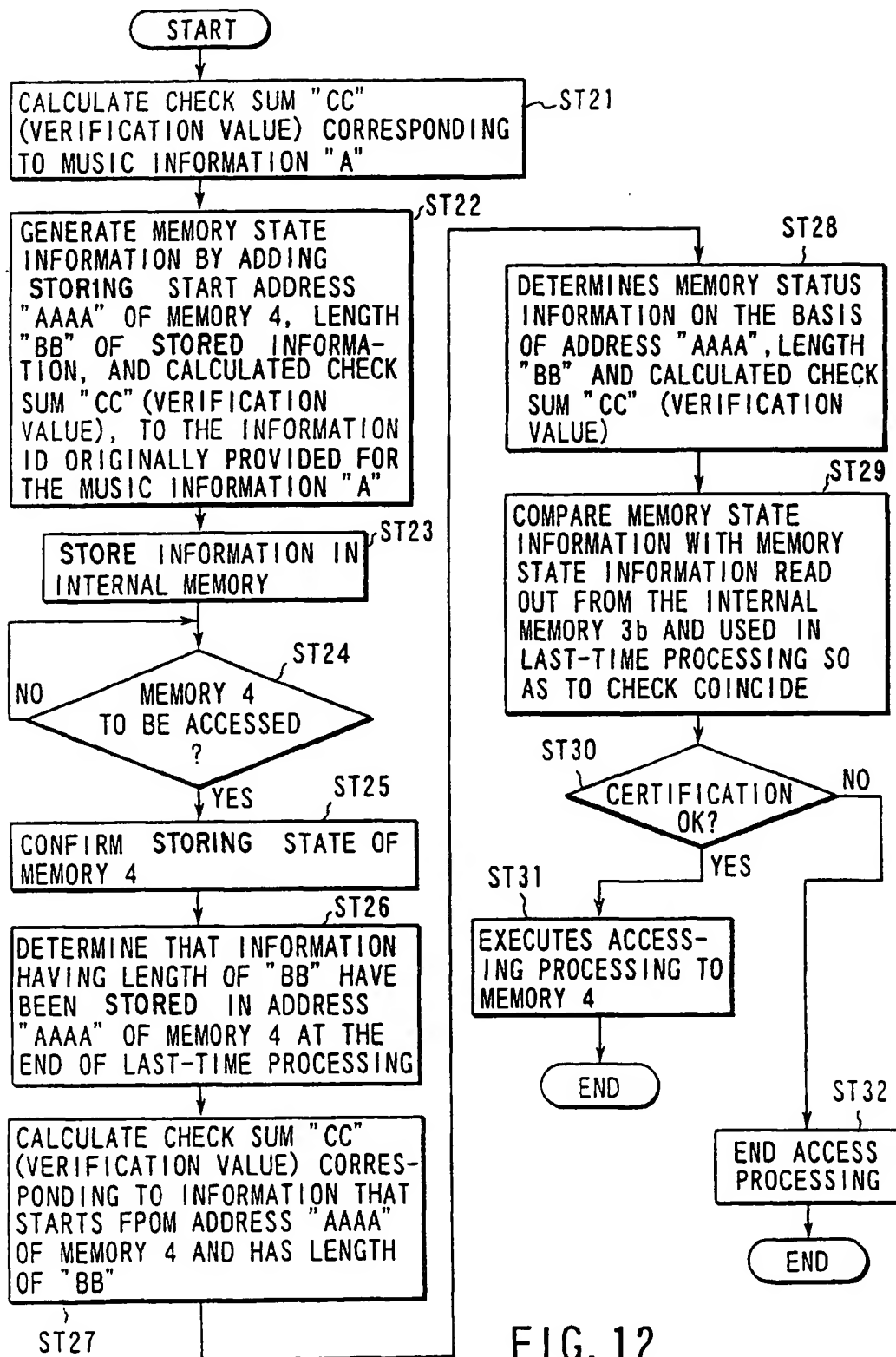


FIG. 12

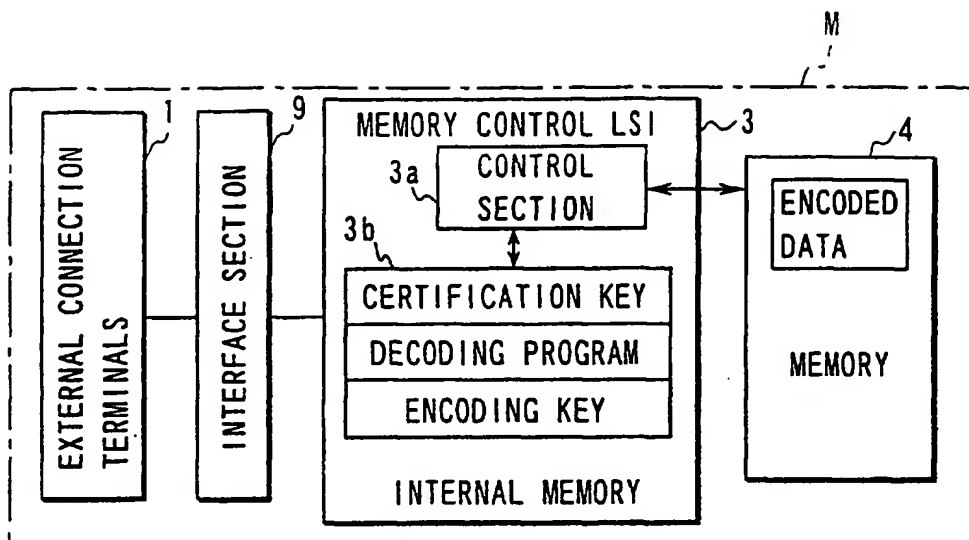


FIG. 14

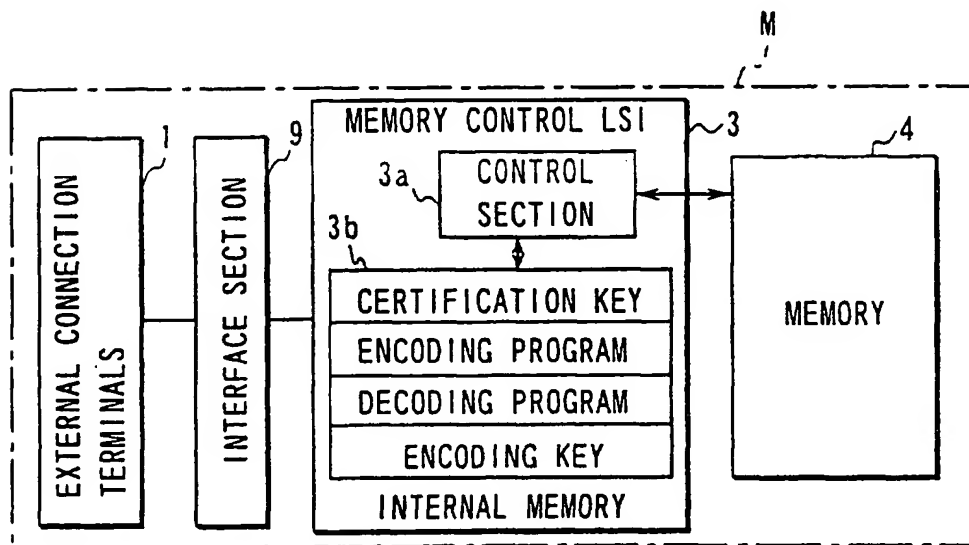


FIG. 17

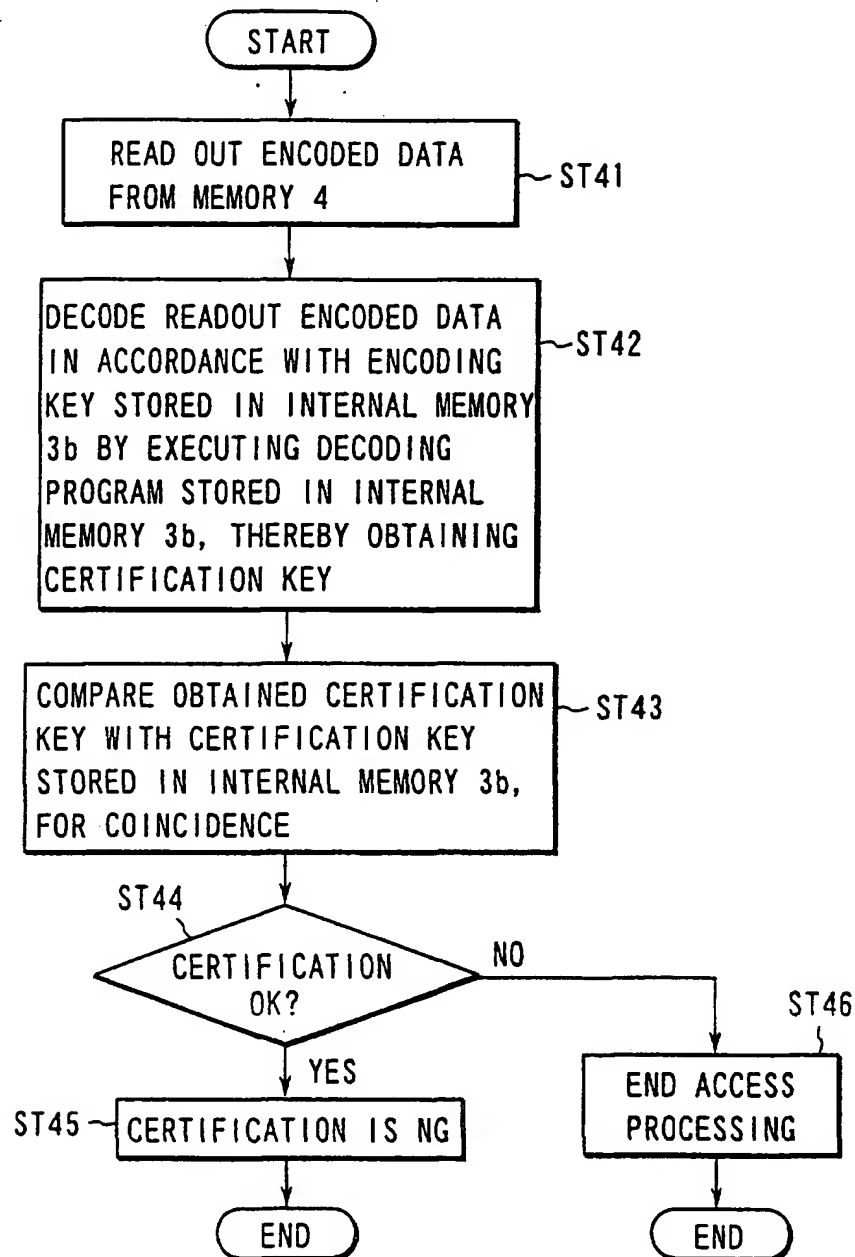


FIG. 15

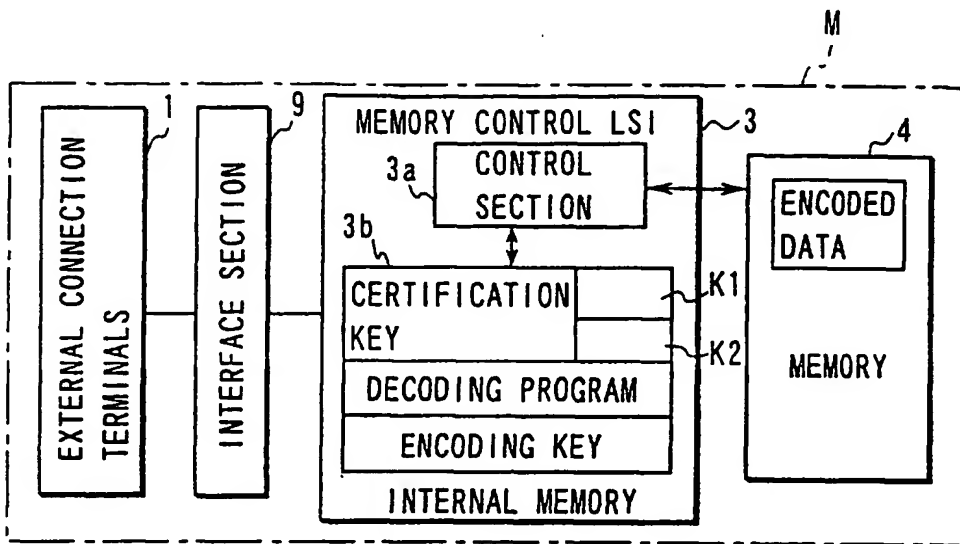


FIG. 16

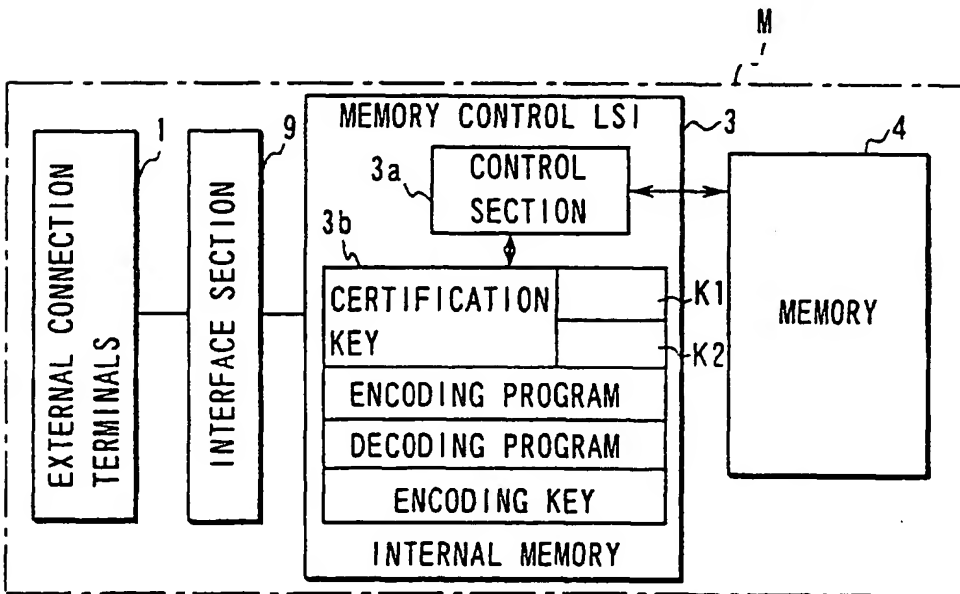


FIG. 19

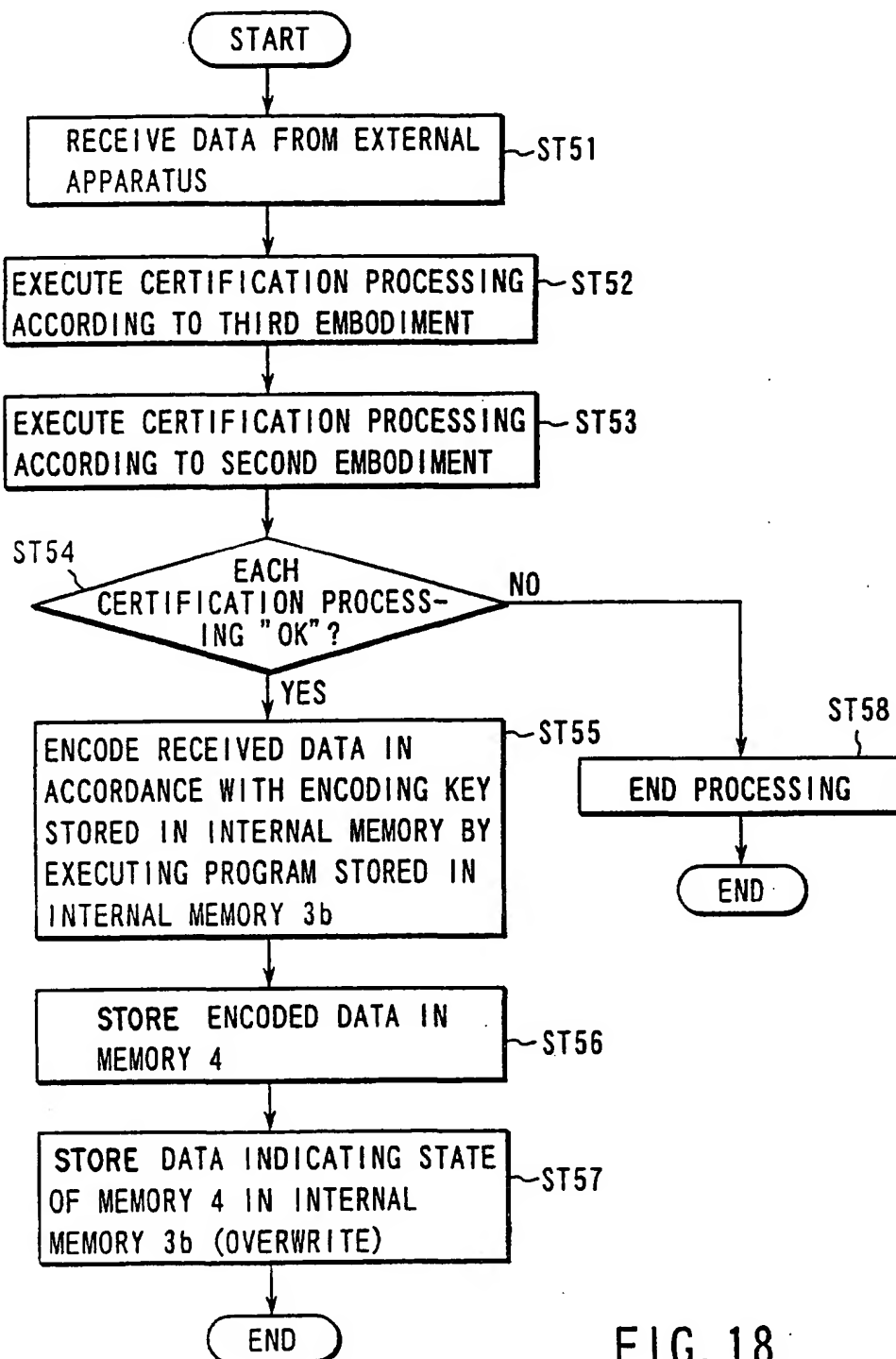


FIG. 18

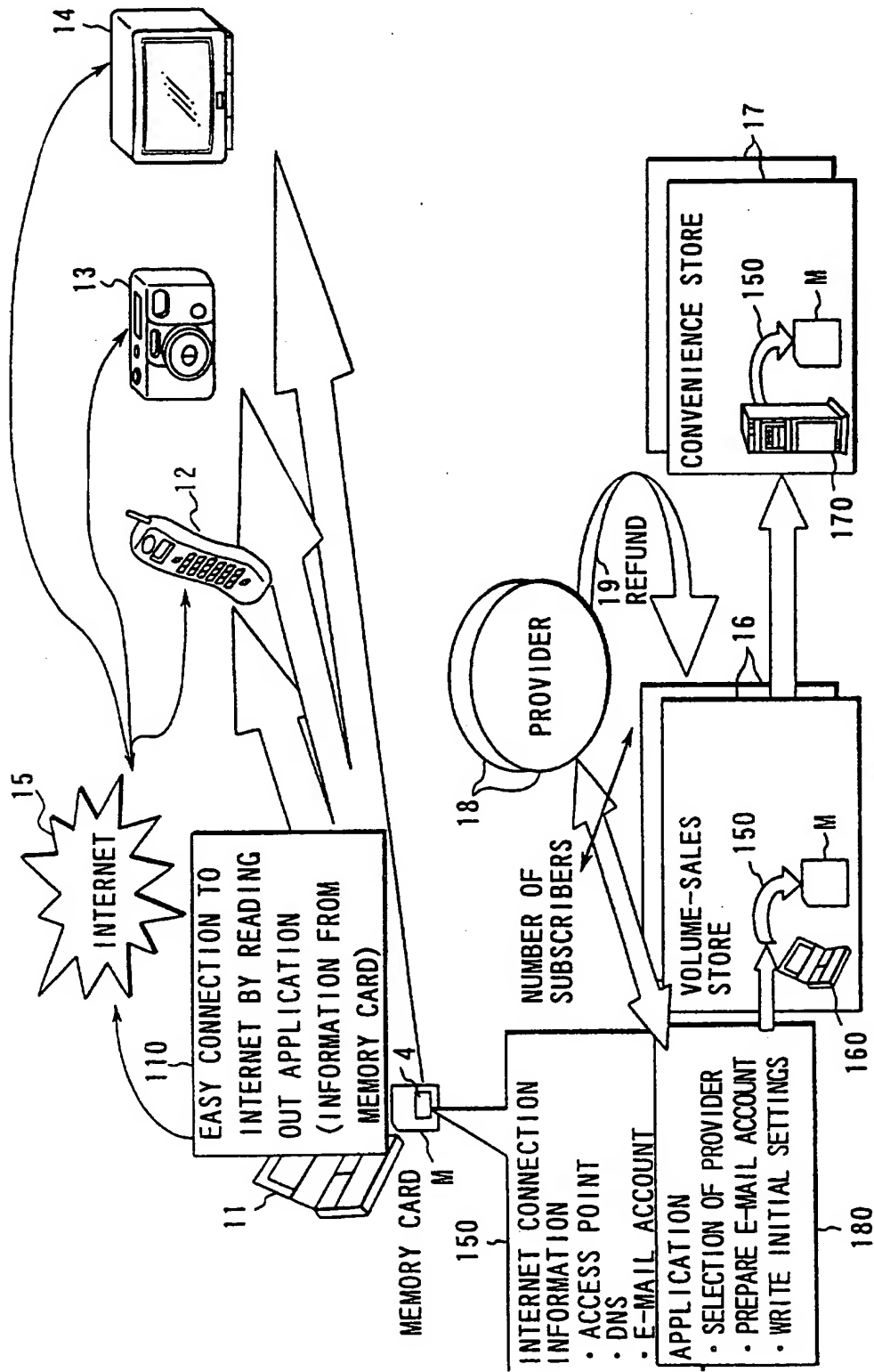
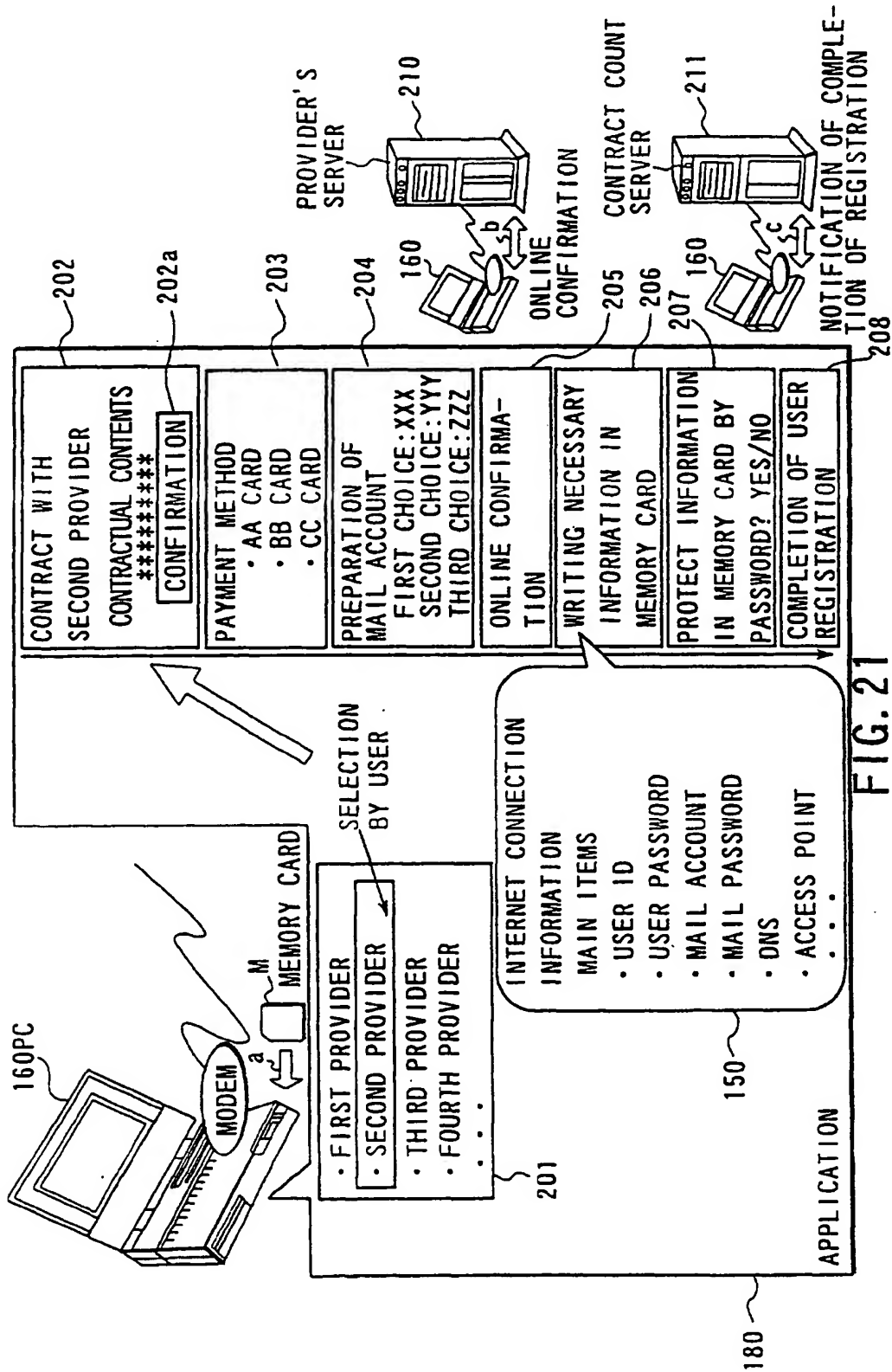


FIG. 20





European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 12 0390

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (InCL7)
Y	WO 98 58305 A (MCCOLL CAMERON; MEMORY CORP PLC (GB); DEAS ALEXANDER ROGER (GB)) 23 December 1998 (1998-12-23) * figure 2 * * page 1, line 19 - page 2, line 30 * * page 5, line 12 - page 10, line 34 * * page 12, line 33 - page 13, line 23 * * page 17, line 4 - line 19 *	1, 2, 6, 15-18, 20	G06F1/00
A	-----	3-5, 7-12, 19	
Y	US 5 838 793 A (LEWIS DAVID OTTO) 17 November 1998 (1998-11-17) * column 1, line 55 - column 3, line 30 * * column 6, line 28 - line 43 *	1, 2, 6, 15-18, 20	
A	US 5 099 516 A (DURKIN MICHAEL D ET AL) 24 March 1992 (1992-03-24) * column 1, line 37 - line 46 *	2	
A	EP 0 911 738 A (CALLUNA TECH LTD) 28 April 1999 (1999-04-28) * column 2, line 17 - column 3, line 7 * * column 3, line 52 - column 4, line 58 *	1, 7, 15	TECHNICAL FIELDS SEARCHED (InCL7) G06F G07F
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 7 February 2001	Examiner Sigolo, A
CATEGORY OF CITED DOCUMENTS X: particularly relevant if taken alone Y: particularly relevant if combined with another document of the same category A: technological background O: non-written disclosure P: intermediate document T: theory or principle underlying the invention E: earlier patent document, but published on, or after the filing date D: document cited in the application L: document cited for other reasons & : member of the same patent family, corresponding document			

EPO FORM 1503 03 82 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 00 12 0390

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

07-02-2001

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9858305	A	23-12-1998	AU 8028798 A	04-01-1999
US 5838793	A	17-11-1998	NONE	
US 5099516	A	24-03-1992	NONE	
EP 0911738	A	28-04-1999	GB 2330682 A	28-04-1999

EPO FORM PUS9

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82